Fortinet FortiGate-100F

Fortinet FortiGate-100F Web Filtering Service User Manual

Model: FortiGate-100F | Brand: Fortinet

1. INTRODUCTION

This manual provides essential information for the setup, operation, maintenance, and troubleshooting of your Fortinet FortiGate-100F 1-Year FortiGuard Web Filtering Service (FC-10-F100F-112-02-12). FortiGuard Web Filtering is designed to protect your organization by blocking access to malicious, hacked, and inappropriate websites, serving as a primary defense against web-based attacks.

Fortinet understands the importance of the Fortinet Security Fabric for your business continuity. FortiCare Services are tailored to meet your deployment and operational needs, regardless of your organization's size or global location.

Figure 1: Fortinet FortiGuard Web Filtering Service Activation Key Package. This package contains the necessary activation key for your service subscription.

2. SETUP

The FortiGuard Web Filtering Service is a subscription-based service that integrates with your FortiGate Next-Generation Firewall. The setup primarily involves activating the service on your FortiGate device.

2.1. Prerequisites

- An active FortiGate-100F device, properly installed and connected to your network.
- Internet connectivity for the FortiGate device to reach FortiGuard services.
- Administrative access to the FortiGate device's web-based manager or CLI.
- The activation key provided with your FortiGuard Web Filtering Service purchase.

2.2. Service Activation

1. Log in to your FortiGate device's administrative interface.
2. Navigate to the **System > FortiGuard** section.
3. Locate the **Web Filtering** service status.
4. Enter your activation key in the designated field and follow the on-screen prompts to register and activate the service.
5. Verify the service status changes to *Active* or *Subscribed*.

For detailed physical installation of the FortiGate-100F hardware, please refer to the separate hardware installation guide provided with your device.

3. OPERATING THE WEB FILTERING SERVICE

The FortiGuard Web Filtering Service enhances your network's security posture by controlling access to web content based on categories and reputation.

3.1. Core Functionality

- **Malicious Site Blocking:** Prevents access to known malicious or hacked websites that could initiate malware downloads or exploits.
- **Content Filtering:** Blocks access to inappropriate or high-risk content based on predefined categories.
- **Threat Intelligence:** Utilizes automated intelligence tools and targeted threat analysis for continuous protection.
- **Policy-Based Control:** Allows administrators to control web access through granular policies configured on the FortiGate device.

3.2. Policy Configuration

To effectively use the Web Filtering Service, you must configure security policies on your FortiGate device. These policies determine which web categories are allowed or blocked for different user groups or network segments.

1. Navigate to **Policy & Objects > IPv4 Policy** in the FortiGate interface.
2. Edit an existing policy or create a new one.
3. Under **Security Profiles**, enable **Web Filter**.
4. Select or create a Web Filter Profile. Within the profile, you can define actions (e.g., block, warn, monitor) for various web categories.
5. Apply the changes and ensure the policy is enabled.

The FortiGuard Distribution Network (FDN) continuously updates web ratings across 6 main categories and nearly 80 micro-categories, allowing for precise policy application and easy management of protection.

4. MAINTENANCE

Regular maintenance ensures the optimal performance and security of your FortiGuard Web Filtering Service.

4.1. Firmware Updates

Ensure your FortiGate device's firmware is kept up-to-date. Firmware updates often include security enhancements, bug fixes, and new features that improve the effectiveness of FortiGuard services.

4.2. FortiGuard Updates

The FortiGuard Web Filtering Service receives continuous updates from the FortiGuard Distribution Network (FDN). Verify that your FortiGate device can reach the FDN servers to receive the latest threat intelligence and web category ratings.

4.3. Policy Review

Periodically review your web filtering policies to ensure they align with your organization's security requirements and internet usage policies. Adjust categories and actions as needed.

5. TROUBLESHOOTING

If you encounter issues with your FortiGuard Web Filtering Service, consider the following troubleshooting steps:

5.1. Common Issues

- **Websites not blocked:**
  Check: Ensure the web filtering profile is applied to the correct security policy. Verify the website's category and that it is set to 'block' in the profile. Check FortiGuard update status.
- **Legitimate websites blocked:**
  Check: Review the web filtering logs to identify why the site was blocked. You may need to override the category or add the site to an allowed URL list.
- **Service not active:**
  Check: Verify your subscription status on the FortiGate device and the FortiCare portal. Ensure the device has internet connectivity to reach FortiGuard servers for license validation.
- **Slow internet access:**
  Check: While web filtering adds processing, significant slowdowns might indicate other network issues or an overloaded FortiGate. Monitor resource usage on the device.

5.2. Contacting Support

If you cannot resolve an issue, Fortinet offers various support services:

- **Device FortiCare:** Provides firmware updates, technical support, and basic FortiGuard subscriptions. Two levels are available: 24/365 support and Advanced Support Engineer (ASE) for faster ticket resolution.
- **Account-Based Services:** Advanced services complementing Device FortiCare, offering designated support engineers and logistics support, along with training and flexible service points.
- **Professional Services:** Provides technical experts for projects, staffing, or other initiatives, available remotely or on-site.

6. SPECIFICATIONS

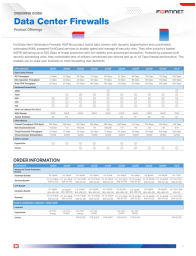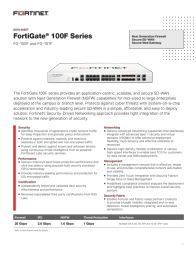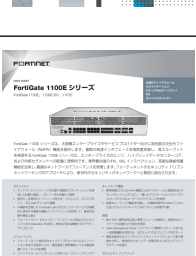| Specification	Value
Brand Name	Fortinet
Manufacturer	Fortinet, Inc.
Product Model Number	FortiGate-5001D
Model Name	FortiGate-100F
Connectivity Technology	Ethernet
Size	1YR Web Filtering
ASIN	B08DQB353W
First Available Date	March 28, 2021
Frequency Band Class	Dual-Band
Compatible Devices	Laptop
Recommended Uses For Product	Security

7. WARRANTY AND PREMIUM RMA

Fortinet offers various options for hardware failure planning and replacement.

7.1. Premium RMA Options

- **4-Hour Parts Delivery:** For situations where space is limited or rapid replacement is critical, parts can be delivered within 4 hours.
- **4-Hour Parts with Engineer:** If physical replacement support is needed, this option includes parts delivery and an engineer to assist with the replacement.
- **Secure RMA:** Available if you wish to self-dispose of the faulty hardware securely.

For specific warranty terms and conditions, please refer to your purchase agreement or contact Fortinet support.

Related Documents - FortiGate-100F

[Fortinet Data Center Firewalls: Ordering Guide and Specifications](#)

Comprehensive ordering guide for Fortinet Data Center Firewalls (NGFWs), detailing product offerings, appliance specifications, order information, and frequently asked questions for high-performance network security.

[FortiGate 100F Series: Next Generation Firewall, Secure SD-WAN, and Secure Web Gateway Data Sheet](#)

Data sheet detailing the Fortinet FortiGate 100F Series (FG-100F, FG-101F), a scalable and secure SD-WAN solution with Next Generation Firewall (NGFW) and Secure Web Gateway capabilities for mid-sized to large enterprises. Features include system-on-a-chip acceleration, advanced threat protection, and comprehensive management.

[FortiOS 7.6.0 Release Notes: New Features, Fixes, and Known Issues](#)

Detailed release notes for FortiOS 7.6.0 from Fortinet, covering new features, enhancements, resolved issues, and known issues for FortiGate network security platforms. Essential reading for administrators and users.

[FortiGate 100F Series QuickStart Guide](#)

A comprehensive guide to installing, setting up, and registering the FortiGate 100F Series network security appliance, including details on interfaces, LEDs, setup options, and licensing.

[FortiOS 7.0.6 Release Notes - Fortinet](#)

Comprehensive release notes for Fortinet FortiOS 7.0.6, detailing new features, resolved issues, known issues, and upgrade procedures for FortiGate network security devices.

[FortiGate 1100E Series Next-Generation Firewall | Fortinet](#)

Fortinet FortiGate 1100E   NGFW   SD-WAN